ID4D
IDENTIFICATION FOR DEVELOPMENT

# Private Sector Economic Impacts from Identification Systems

WORLD BANK GROUP

# Contents

# Tables



# Figure

# About ID4D

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from World Bank Group, Bill & Melinda Gates Foundation, and Omidyar Network.

To find out more about ID4D, visit worldbank.org/id4d.

# Acknowledgments

This report was prepared in 2018 by One World Identity (OWI) as part of the Identification for Development (ID4D) initiative, the World Bank Group's cross-sectoral effort to support progress toward identification systems using 21st century solutions. It was made possible through the generous support of the partners of the ID4D Multi-Donor Trust Fund (Bill & Melinda Gates Foundation and Omidyar Network).

OWI is an independent identity research and strategy company focused on cybersecurity, digital commerce, and risk management. They help businesses, investors, and governments stay ahead of market trends so they can build sustainable, forward-looking identity-enabled products and strategies.

The OWI team that contributed to this paper include: Kaelyn Lowmaster (author) and Dasha Cherepennikova (contributor). This report benefited greatly from the inputs and reviews of the World Bank Group staff including Julia Clark, Luda Bujoreanu, Kamya Chandra, and Jonathan Marskell, under the supervision of Vyjayanti Desai.

In addition, this report would not have been possible without the insights and reviews by Aubra Anthony, Jim Barnett, Pascal Bouvier, Jeremy Grant, Arthur Henderson, Phil Lam, Emma Lindley, Balazs Nemethi, Kyla Reid, Anneke Schmider, Hüseyin Tanriverdi, Yiannis Theodorou, Don Thibeau, Jonathan Williams, Steve Wilson, and Kaliya Young.

# Abbreviations

| | |
|---|---|
| AML | Anti-money laundering |
| API | Application programming interfaces |
| CNIC | National ID Card (Pakistan) |
| eKYC | Electronic know your customer |
| EU | European Union |
| FTC | Federal Trade Commission (US) |
| FVS | Facial Verification Service (Australia) |
| GDPR | General Data Protection Regulation (European Union) |
| KYC | Know your customer |
| NADRA | National Database and Registration Authority (Pakistan) |
| NIDS | National Identity System (Jamaica) |
| NGO | Nongovernmental organization |
| PPP | Public-private partnership |
| RITA | Registration, Insolvency and Trusteeship Agency (Tanzania) |
| SSN | Social Security Number (United States) |
| UAE | United Arab Emirates |
| UIDAI | Unique Identification Authority of India |

# Executive Summary

Identification systems are a core component of sustainable development policies in countries with diverse economic, demographic, and political contexts. Robust identification systems with widespread coverage can—particularly when digital—produce a wide array of advantages for governments and individuals, including facilitating access to benefits, rights, and services, and improving public administration, planning, and service delivery. In addition, preliminary evidence suggests that identification systems can provide a number of fiscal benefits for the public sector, including decreasing fraud and leakage in transfer programs, increasing administrative efficiency, improving tax collection, and providing additional sources of revenue.[1]

The role of digital identification systems in the private sector is equally large. In order to transact with customers and provide services, many companies—including those that provide banking and financial services, mobile operators, digital commerce platforms, airlines, and more—must verify and authenticate the identities of their users at various points in the customer lifecycle. The source of validity for customer identity is often a government-provided or recognized credential, such as a national ID, passport, or other document. Where authoritative proof of identity is scarce, companies are likely to have smaller available customer pools, higher administrative overhead, and greater risks of fraud.

To date, however, rigorous research and reliable data measuring these impacts are scarce. This paper is intended to begin filling this gap by providing a summary of existing evidence and an analytical framework to consider the cost savings and revenue generation opportunities that government-provided or recognized identification systems can create for the private sector. Building on the approach of World Bank's Identification for Development (ID4D) companion paper on public sector savings and revenue, it highlights five key **features of identification systems** that are most impactful for the private sector, including:

- **Digitization.** The transition from paper-based to digital systems throughout the identity lifecycle can reduce private sector operating expenses and transaction costs.
- **Unique ID.** The creation of a unique identifier for each individual within the population can increase transaction efficiency and reduce opportunities for fraud.
- **Integration and Interoperability.** The integration, interoperability, or dependency between identification systems can increase transaction efficiency, facilitate digital queriability by private sector firms, and reduce opportunities for fraud.
- **Queriability for Verification and Authentication.** The ability of private sector companies to efficiently, securely, and consistently query an identification system for information can increase transaction efficiency and facilitate effective private sector verification and authentication processes.
- **Public-Private Partnerships (PPPs).** Direct private sector participation in the architecture and continued execution of national-level identification systems can increase transaction efficiency and enable private sector revenue generation for identity-related services.

When identification systems have sufficient coverage, robustness, and accuracy, each of these features has the potential to positively impact private firms through three primary **economic channels:** (1) decreasing

1 World Bank. (2018). "Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints." Washington, DC: World Bank Group, available at http://www.worldbank.org/en/programs/id4d.

costs and expenditures, (2) increasing revenue, and (3) improving the overall business climate. Although evidence is limited, these channels are illustrated by a handful of case studies from a variety of countries and sectors, including financial services, mobile and telecommunications, and the travel industry:

- **Savings Channel.** Identification systems can create opportunities for private companies to decrease costs and expenditures along a variety of dimensions, including:
  - *Reduced administrative and transaction costs.* The transition from a paper-based identification system to a digital one that provides a unique ID and/or queriability can save firms substantial money in onboarding costs and other identity verification or authentication transactions throughout the customer lifecycle. In India, for example, the typical firm's onboarding cost has been about 1,500 rupees ($23). With the increased queriability, digitization, and interoperability of the Aadhaar system, some estimate that onboarding costs could plummet to as little as 10 rupees ($0.15).
  - *Reduced theft and fraud.* By limiting the potential for identity theft and helping companies more accurately gauge customer risk, robust identification systems with high levels of accuracy, queriability, integration, and/or interoperability can help reduce company losses due to theft and fraud. Such systems are crucial for combating threats like synthetic identity fraud, which is anticipated to cost lenders worldwide approximately $6 billion per year.
  - *Reduced compliance costs.* Queriable identification systems with high levels of data accuracy can also help firms reduce compliance costs—such as those associated with know your customer (KYC) and anti-money laundering (AML) regulations—by increasing the ease and security of identity verification and authentication. In Europe, for example, KYC costs the average bank $60 million per year, with individual transactions ranging from $13.40 to $134 per identity check.
  - *Reduced liability costs.* The liability costs associated with collecting, storing, and disposing of personal data are potentially high. The European Union, for example, has recently passed a law that will impose a maximum penalty of €20 million ($23.63 million) or 4 percent of global annual turnover from the previous year, (whichever is greater) on companies that fail to adequately protect identity data. To the extent that firms can use external identification systems to minimize the personal data they hold, they may be able to lower these costs.
- **Revenue Channel.** Robust, widely used identification systems can also facilitate increased revenue levels and revenue generation opportunities for private firms across industries, including through:
  - *Increased identifiable consumer base.* The lack of identity documents is a concrete barrier to access public and private services that require proof of identity. Increasing the coverage of robust identification systems therefore has the potential to increase the customer base of firms in a variety of industries. In Pakistan, for example, Telenor was able to leverage the national ID and government-mandated SIM registration to expand the customer base for its Easypaisa payments service, which now has 20 million users and processes the equivalent of 3 percent of Pakistan's GDP.
  - *Decreased consumer abandonment and rejection.* By reducing the transaction costs that consumers face when verifying or authenticating their identities, digital, interoperable, and queriable identification systems can help reduce customer abandonment. Furthermore, when such systems help companies more accurately gauge risk, they not only help prevent fraud, but also decrease the number of false positives (low-risk customers falsely assigned a high-risk score) and rejected transactions due to inaccurate verification. In the U.S. online retail market, for example, companies lose $118 billion in revenue in a given year due to unwarranted transaction rejections, as compared to $9 billion in measured fraud.

- *Fees charged for identity-related services.* An additional opportunity for revenue generation in the private sector results from the ability of firms directly involved in providing government-recognized identification systems—i.e., through a partnership or PPP—to charge fees for identity services. This has the potential to create revenue streams both from per-transaction fees themselves and from add-on services.

- **Economic Climate Channel.** Finally, identification systems can play an instrumental role in achieving the Sustainable Development Goals[2] by contributing to inclusive growth that benefits the broader economy. In addition, these systems can help underpin digital development strategies, creating a "business friendly" environment for companies. In Estonia, for example, a robust digital identification system has enabled the country's innovative e-Residency program, which has led to the creation of more than 1,300 new companies by e-Residents, bringing an additional $4.6 million into the Estonian economy.

This paper is a first step toward holistically evaluating the potential shared benefits of identification for the broader economy. By aggregating existing case studies and identifying specific impact channels, it provides a preliminary assessment of the economic relationship between government-backed identity systems and private sector firms across multiple industries. As a result, we hope that this paper will serve as a resource for governments, donors, private sector leaders, and industry groups to fruitfully engage on issues related to identity, and a point of departure for more rigorous research on this topic.

2 See "Principles on Identification for Sustainable Development: Toward the Digital Age." World Bank, 2017.

# 1. Introduction

Identification systems are a core component of sustainable development policies in countries with diverse economic, demographic, and political contexts. Robust identification systems with widespread coverage can—particularly when digital—produce a wide array of advantages for governments and individuals, including facilitating access to benefits, rights, and services, and improving public administration, planning, and service delivery. In addition, preliminary evidence suggests that they can provide a number of fiscal benefits for the public sector, including decreasing fraud and leakage in transfer programs, increasing administrative efficiency, increasing tax collection, and providing additional sources of revenue.[3]

The role of digital identification systems in the private sector is equally large. The efficient, accurate, and secure use of personal identity data is at the heart of most transactions, regardless of the industry in which they take place. At a very basic level, any exchange of value between a user and a service provider typically requires each side to know, with some degree of confidence, with whom they are interacting. This knowledge of a customer's identity is particularly salient and highly regulated in some industries, as with mandated know-your-customer (KYC) and anti-money laundering (AML) protocols in financial services, or where proof of identity is mandatory to register a prepaid mobile SIM card.[4] In other contexts, identity-related processes may be less formalized, but are still fundamental for completing transactions such as paying one's mobile phone bill, taking out an insurance policy, or making an online purchase.

The source of validity and authority for these transactions is often a government-provided identity credential, such as a national ID card or number, passport, or birth certificate. Where such credentials are unavailable, individuals are often excluded from large portions of the formal economy. Currently, 1.1 billion people worldwide lack proof of legal identity.[5] This untapped customer base translates to sizable economic inefficiencies that can hamper market growth across sectors. From a service provider perspective, a lack of authoritative identities means that companies must rely on expensive manual verification procedures for identity proofing, burdensome in-person transactions, and cash-based exchanges. In some cases, they may invest in ad hoc identification systems for internal use. In other cases, a company may simply be unable to provide services for customers who have no way to prove their identities. Where authoritative, government-recognized identity credentials are scarce, companies are likely to have smaller available customer pools, higher administrative overhead, and greater risks of fraud.

The implementation of robust and inclusive identification systems at the national level therefore offers the potential for large financial gains for private sector companies. However, as with the public sector, evaluating the direct economic effects of identification systems on private firms is challenging. As a companion piece to the World Bank's Identification for Development (ID4D) work on fiscal savings for government agencies, this paper provides a first step toward developing a greater understanding of the financial benefits of identification systems for the private sector. By developing a framework for cost savings and revenue generation opportunities and aggregating existing case studies, it provides a preliminary assessment of expected benefits of government-backed identification systems for firms across a variety of industries. This paper is therefore intended to serve as a resource for governments and donors looking to gauge the

3 World Bank, 2018.

4 For more information on legally-mandated mobile SIM card registration, see https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards.

5 For more information on identification around the world, see http://www.worldbank.org/en/programs/id4d.

potential impacts of implementing an identification system and for private sector leaders and industry groups to fruitfully engage on identity-related issues. We hope it will also serve as a point of departure for future quantitative modeling on this topic.

# Approach

## Challenges with Evaluating Financial Impacts

Evaluating the economic impacts of identification systems for both the public and private sector faces two common challenges. First, comprehensive data sets are scarce, either because governments and companies have not systematically monitored fiscal impact as part of identification system implementation, or because the underlying data collection methodology is opaque, anecdotal, or based on unreliable assumptions. Second, the wide variation in identification systems across countries makes comparisons across cases difficult. Isolating the causal impact of identifications systems will require more data and additional methodological attention in future research efforts.

Two additional obstacles are particularly relevant to private sector analyses of this topic. First, the far-reaching and diffuse nature of effects in the private sector presents greater issues for data collection. Because identity touches nearly every transaction that involves an exchange of value or trust, potential cost-savings mechanisms could be identified for nearly every industry in any given jurisdiction. Relying exclusively on more abstract measures of GDP growth or "ease of doing business" as a proxy for private sector impact may capture the expansiveness of impact and overall benefit to national development goals, but also sacrifice a more precise understanding of impact mechanisms that would be useful to inform future policy choices.

Second, fiscal impacts on the private sector are, in many cases, second-order effects of a government's decision to implement or reform an identification system. Given that the primary goal of these systems is typically to pursue public policy objectives—e.g., improving service delivery, streamlining public administration, increasing security, etc.—measuring the impact on the private sector has not typically been prioritized. Nonetheless, governments should not discount the very real potential benefits to their broader economies when crafting an identification system, even though this broader class of private sector benefits have thus far remained relatively unexamined.

## Methodology and Scope

To address these obstacles, this paper builds on the approach presented in World Bank (2018). It first outlines the features of government-provided identification systems most likely to produce significant private sector impact, and then provides an overview of specific channels through which these features may have economic impacts. Specifically, it focuses on digital, "foundational" identification systems: those created to provide proof of identity for a wide variety of purposes, and including but not limited to national ID cards, unique ID numbers, and population registers.[6] With that framework in place, this paper then illustrates the potential impact channels of such identification systems through both industry-specific and geographic lenses.

In addition, the focus of this paper is on the second-order benefits of *existing* identification systems to private firms across industries. As such, it does not consider revenue *directly generated* by identity solution vendors that provide software, hardware, credentials, database integration, and other inputs into the *creation* of government identification systems. Section 3 does, however, analyze the interplay between

6 Throughout the remainder of this paper, the term "identification system" therefore implies a *foundational* system provided or recognized by the government, unless otherwise specified.

private and public entities in jointly administered identification systems, along with revenue generation opportunities created by public-private partnerships (PPPs).

As with its public-sector companion piece, this paper does not seek to provide a quantitative model of identity-related savings or revenue generation in the private sector. More targeted analysis will be required to determine causality of various drivers and the generalizability of benefits across cases. However, by providing an early evidence base and analytical framework, the intent is to construct a foundation for future predictive models.

## Organization

Section 2 of this paper provides an overview of the core components of an effective, impactful identification system, building on the companion public-sector savings piece.[7] With these variables in mind, Section 3 explores the primary channels through which these systems can decrease expenditures, generate revenue, and foster broader market development. This section also includes industry-specific and geographic case studies that illustrate the interplay of various economic impact channels. Section 4 offers conclusions and suggestions for further research.

7 World Bank, 2018.

# 2. Key Features and Conditions of Identity Systems

Identification systems vary along multiple dimensions according to purpose, cultural context, system architecture, governance, enrollment mechanisms, and data collected. To address this heterogeneity, this paper adopts a features-based approach to examine the role of identification systems for the private sector. The type and scale of economic impacts for the private sector are products both of explicit system features and implementation choices, as well as broader conditions including system coverage and robustness. Here the goal is not to draw a direct correlation between particular features and the magnitude of economic impact, but rather to illustrate the tools available to governments as they prioritize investment in identification systems.

## Key Features of Identification Systems

This section discusses particular features of identification systems that emerge as the result of explicit choices made by system architects. The four primary features that impact public sector savings and revenue[8]—digitization, a unique ID, integration and interoperability, and digital authentication—also matter for private sector savings and revenue generating opportunities. In addition to viewing these four through a private sector lens, this section expands the "digital authentication" feature to include the concept of "queriability" to facilitate digital verification and authentication processes. It also presents an additional feature—direct private sector participation in the management of identification systems—that has obvious economic impacts for private industry.

### Digitization

"Digitizing" an identification system refers to the process of transitioning from legacy paper-based systems (or, in some cases, the absence of a system entirely) to electronic records and processes. Digitization is a key component of cost savings throughout an individual's "identity lifecycle" in the public sector—that is, from the time a person is enrolled and created as a unique entry within a given system, through that identity's use in verification and authentication procedures, to the continual maintenance of identity information databases to ensure dynamic correctness over time, even as an individual's attributes change.

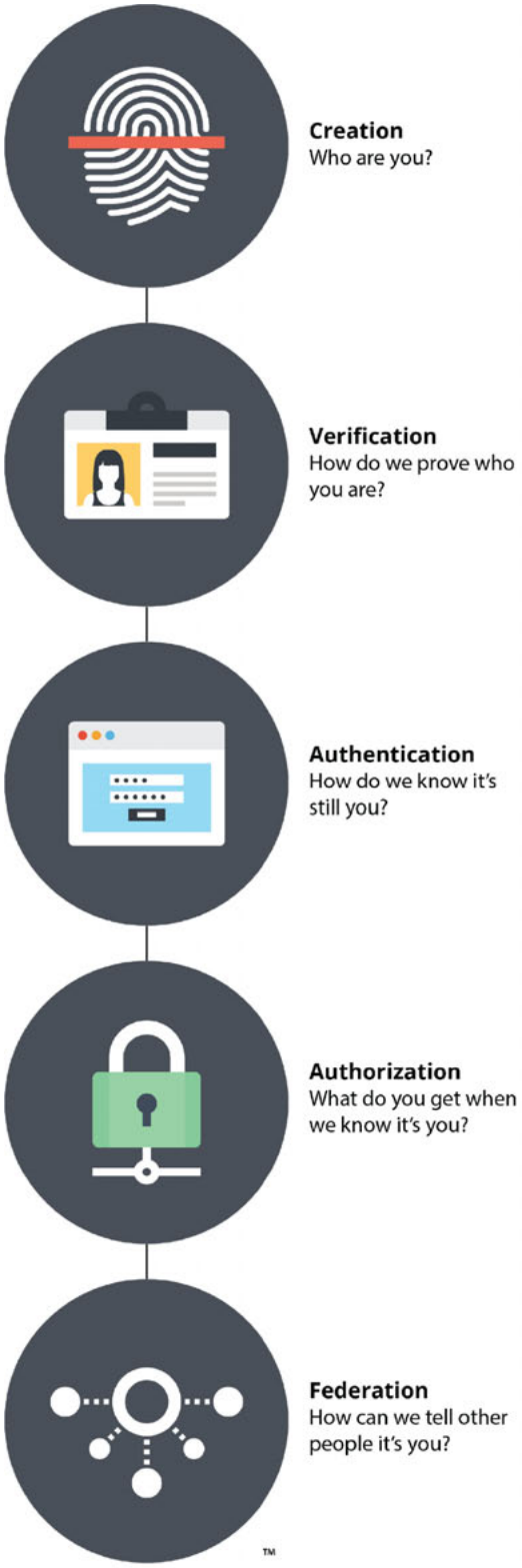
8 See World Bank, 2018.

**Table 1: Savings and Revenue Generation Features of Identification System Design for the Private Sector**

| Feature | Description | Key Benefits |
|---|---|---|
| **Digitization** | transition from paper to digital-based systems, including of databases, credentials, data transfer, etc. | • *Direct:* reduces operating and transaction costs<br>• *Indirect*: enables unique ID, integration, digital authentication |
| **Unique ID** | creation of a unique identifier –often biometric-based–for each member of the target population | • *Direct:* increases transaction efficiency; reduces fraud opportunities<br>• *Indirect*: enables integration and queriability |
| **Integration and Interoperability** | connections between different identification systems, including their ability to exchange information | • *Direct:* increases transaction efficiency; facilitates queriability; reduces fraud opportunities<br>• *Indirect*: incentivizes system adoption by incorporating a wider array of services into a given identity platform; encourages positive network effects |
| **Queriability for Verification and Authentication** | the ability of private sector companies to efficiently, securely, and consistently query and identification system for information | • *Direct:* increases transaction efficiency; facilitates effective private sector verification and authentication<br>• *Indirect:* reduces private data liability costs; mitigates fraud opportunities; incentivizes value added services; encourages positive network effects |
| **Public-Private Cooperation and Partnerships** | the extent to which private sector companies are directly involved in the architecture and continued execution of identification systems | • *Direct:* enables private sector revenue generation for identity services |

Over the past decades, many countries have digitized their identification systems, with concrete benefits for private sector companies that rely on these systems throughout the identity lifecycle they manage for their customers (see Figure 1). In financial services, for example, a new customer must first be "onboarded" to a particular company, a process which may involve verification of authoritative identity credentials to minimize counterparty and fraud risk, as well as to satisfy any relevant KYC and AML procedures that apply in that jurisdiction. A newly onboarded customer may then be authenticated with each use of the company's services, as with logging into a bank account online. Ensuring dynamic correctness of an individual's identity information over time is necessary to ensure that a customer is authorized to access appropriate attributes of a company's services. In some cases, a customer's digital identity with a

## Figure 1: Identity Lifecycle Building Blocks for the Private Sector




*Source:* One World Identity (OWI).

particular private sector institution can be federated—that is, shared with other service providers in order to access a greater variety of private sector services.[9] In Norway's Mobile BankID program, for example, a shared infrastructure between the country's largest mobile provider and dozens of participating banks allows for federation of identities for authentication across a huge array of services in both the public and private sectors.[10]

If no digital system exists for cross-checking government records held by different agencies, a corporation may be required to invest employee time and company resources to establish assurance through paper-based inquiries, in-person visits, or call center engagements, all of which are more costly transactions than internet-based inquiries. A trusted digital identity reduces the time and material required to conduct initial onboarding, can speed subsequent authentications and reduce unauthorized access to services, and can be portable across sectors, services, and use cases.

## Unique ID

A fundamental attribute of robust identification systems is not only the ability to establish the *existence* of individuals in a given jurisdiction, but also their *uniqueness*. In many cases, this involves providing individuals with a national identification number (NIN), registered in conjunction with other personally identifying information like name and date of birth. In a growing number of cases, countries have relied on biometric attributes such as fingerprints and iris scans to increase the accuracy of identity databases and ensure statistical uniqueness.

Such systems can be useful to private sector companies who also rely upon unique identifiers to facilitate reliable onboarding procedures and to avoid errors and fraud throughout a customer's life cycle with a given company. If a firm is able to confidently leverage a unique identification system at the outset of its relationship with a customer, it can preserve resources it would otherwise have spent endogenously determining the unique identity of that customer. As the customer-service provider relationship continues, that same unique identifier can help ensure that a customer is differentiated from another entity sharing some elements of personally identifying information (i.e., that the purchases of Jane Doe with NIN 12345 are not mistakenly reflected on the credit record of a different Jane Doe, NIN 13245). In cases where misattribution or misidentification cause customer losses, the burden of redress typically falls upon the private sector firm that completed the erroneous transaction. A robust, unique identification system can mitigate such costs.

## Integration and Interoperability

Governments normally operate multiple databases and registers to manage identity data for the population within their borders for a variety of purposes. This often includes, for example, a national ID system, civil registration, voter registers, a tax identity system, databases of social security beneficiaries, and more. Where these systems are highly fragmented and non-interoperable, databases are likely to be duplicative and inconsistent, and individuals may hold and use a variety of identity credentials as proof of ID, enabling fraud and increasing the burden of identity verification. In contrast, integrated and interoperable systems streamline identity management and offer a common entry point—e.g., a national ID or unique ID number—for establishing, verifying, and authenticating an individual's identity.

Whether a country's identity ecosystem is fragmented or integrated has implications for public sector savings, but also for the cost of identity verification for the private sector. Where no single trusted identifier

9 For more information on distinct identity use cases throughout the private sector identity lifecycle, see "Don't Believe The (Blockchain) Hype: The Definitive Primer on Identity and Blockchain." One World Identity, July 2017.

10 See "Norwegian Mobile BankID: Reaching scale through collaboration." GSMA, 2014.

exists, a private corporation may be required to individually query multiple existing databases to build a comprehensive customer profile, establish counterparty trust, and minimize the risk of default or fraud. A system that reduces these redundant efforts would present a significant value proposition for private companies, facilitating higher levels of system adoption and enrollment. This "virtuous cycle" of adoption will be discussed in more detail in the section on coverage rates below.[11]

Moreover, lack of integration and interoperability between government identification systems creates a range of potential avenues for fraud based on the exploitation of discrepancies between records. When this fraud is perpetrated in private sector transactions, the private sector bears not only the burden of onerous and inefficient record checks at the initiation of a customer relationship, but also the financial burden of redress in the event of fraud.

## Digital Queriability for Verification and Authentication

Another important feature of government-backed identification systems is their ability to facilitate digital verification and authentication services. In many instances, these processes are limited to transactions between public sector agencies. Others, however, offer direct mechanisms by which private companies can also interact with the system to confirm identity information for various use cases. Where these private sector queries are possible, a new driver of economic impact emerges.

"Queriability" is a term used in this paper to capture this characteristic of identity systems. Queriable systems allow for efficient, secure, and consistent information requests originating from private sector companies.[12] Queriability multiplies the potential economic effects of an identity system on the private sector in several ways. First, particularly with the rise of digital and mobile financial services, an easily queried identification system can drastically lower transaction costs when corporations require a high degree of identity assurance. Second, where costs to query government systems are low,[13] high queriability can provide an incentive for private companies to build value-added services. This, in turn, may encourage customer enrollment in the identification system, further boosting coverage rates and overall system robustness. Queriability also allows private organizations to reduce the number of customer attributes held for the purposes of identification,[14] which poses a considerable security and liability risk.

Conversely, identification systems with a low degree of external queriability can give rise to additional costs via increased fraud risk or requiring companies to turn to third-party verification providers. With synthetic identity fraud, for example, malicious actors combine attributes (e.g., name, ID number, and

---

11 While establishing interoperability—both internally between siloed government systems and externally through private sector query platforms—constitutes a primary economic impact channel, it may also raise questions of privacy and user consent. In Australia, for example, recent efforts to integrate Medicare cards as a means of verification in the country's Govpass digital identity platform provoked an outcry from privacy advocates. This came after an announcement that Australia's Facial Verification Service (FVS), a database of citizen photos which underpins Govpass, would expand to include all citizen passport photos. Govpass is voluntary, but the FVS is not. Other cultural contexts may lead to varying levels of tolerance for data sharing through database linkages, but governments should prioritize legal protections to ensure the economic efficiencies of database harmonization are not outweighed by the risk of privacy violations or data misuse. These issues are discussed in more detail in World Bank (2018).

12 Constructing a queriable system does not mean, however, that companies have unrestricted access to personally identifiable information held in government records. Some countries with foundational systems have constructed Application Programming Interfaces (APIs) by which companies requiring verification or authentication of a customer's identity can query existing government systems, and in turn the government identity authority can confirm the veracity of a desired set of attributes.

13 See Section 3 of World Bank (2018) for a detailed discussion of fees charged by governments for identity services.

14 Most companies will still likely hold some amount of personal data about customers or prospective customers to facilitate service delivery, payment processing, marketing, and other business functions.

address) of multiple real people to create new, fictional identities.[15] Protecting against this relatively new class of fraudulent activity and ensuring that identity credentials actually belong to the person presenting them requires interoperability and/or integration between systems and a high degree of queriability.

## Direct Private Sector Participation in Identity System Architecture

To date, most government-led identification systems have used traditional procurement methods to purchase various identity-related inputs (e.g., hardware, software, credentials, systems integration, etc.). Given that revenue from these contracts is the core model of identity solutions providers, they are not included in this paper. In some cases, however, the private sector is directly involved in the architecture of systems themselves, administering either wholly or in part the creation, implementation, and integration of national-level systems.[16]

The United Kingdom's GOV.UK Verify system, for example, allows users to access public sector services online after their identity is verified by a private sector company of the user's choice, like Barclay's or Experian.[17] In Canada, SecureKey Concierge follows a similar model with several tier one financial institutions serving as identity providers for citizens to access more than 80 government services.[18] Many emerging cases of this type are built on preexisting identity verification processes as part of KYC and onboarding in the financial services and mobile sectors. They can then be adopted for public sector use cases, or jointly managed as a PPP in pursuit of either foundational or functional goals. This creates the potential for even more immediate private revenue generation and savings opportunities.

Direct private sector participation in identification system architecture can have particularly targeted economic impacts. Depending on the policy framework in which a given system is constructed, the costs of integration may be able to be shared between the public and private stakeholders. Private companies that provide identity services, such as digital verification and authentication, may also charge user fees to public agencies for a variety of use cases, generating a potential new revenue source.[19]

It is important to note, however, that despite the potential benefits of a partnership to both the public and private sectors—such as lower up-front investment costs for governments and potential revenue streams for firms—these arrangements also come with certain risks. This includes, for example, the potential for vendor lock-in, which typically raises the overall costs and reduces the long-term flexibility and innovation of the identification system. Similarly, to the extent that fee charging models pass prices onto consumers, this can raise the cost of identification systems, potentially making them cost prohibitive and working against the goal of identification as a universal public good.

---

15 See, for example, https://www.wsj.com/articles/the-new-id-theft-thousands-of-credit-applicants-who-dont-exist-1520350404.

16 For a more detailed description of common types of public-private partnerships in identification systems, see "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. A joint World Bank Group—GSMA—Secure Identity Alliance Discussion Paper," World Bank, 2017.

17 For a full list of identity providers in the GOV.UK Verify network and more information about the program, see Corfe, Scott, "A Verifiable Success: The Future of Identity in the UK." The Social Market Foundation, August 2017.

18 See "Building Canada's Digital Identity Future." Digital Identification and Authentication Council of Canada, May 2015, for more information.

19 It is worth mentioning that many private, digital identity verification processes that are adopted for public sector use or incorporated into an identity-related PPP are still likely to rely on some form of government-recognized identity credential. Many countries, for example, require a national ID to be presented in order to activate a SIM card, after which an individual's mobile digital identity can provide federated verification and authentication to additional services (see Pakistan Case Study snapshot in Section 3). Thus, the economic impacts of private sector participation in an identification system are likely to be magnified where a robust identity credential with high coverage already exists, and mitigated where such infrastructure has not yet been created. For more information on effective regulatory sequencing and policy integration, see GMSA, "Regulatory and policy trends impacting Digital Identity and the role of mobile: Considerations for emerging markets," October 2016.

# Additional Conditions Affecting Economic Impact

Beyond the features described above—which are largely determined by system design—there are several other identification system characteristics that influence potential cost savings and revenue generation opportunities for the private sector. These include the number of individuals covered by a particular identification system and the robustness and accuracy of data collected over time.

## Coverage Rates

Coverage rates—the percentage of the population within a given jurisdiction whose information is included in an identification system—are one of the fundamental determinants of a system's effectiveness. An estimated 1.1 billion people do not have a proof of their legal identity,[20] and the lack of identity documents is highly correlated with poverty levels both between and within countries. Without substantial coverage rates, a system simply cannot deliver the development benefits for which it was designed.

From a private sector perspective, low enrollment levels are perhaps the greatest obstacle to economic impacts across industries. When a private sector corporation cannot rely on high coverage, high confidence, government-recognized identities, it will often be forced to turn down otherwise qualified customers due to lack of counterparty information, thereby sacrificing potential revenue gains and drastically narrowing customer pools. It may also incur elevated administrative and onboarding costs as a consequence of costly endogenous, manual, or in-person verification processes.

Anecdotal research has indicated that coverage rates below 50 percent are of limited operational use, but once systems reach 80 percent of the population or more, they tend to generate a cumulative effect as both private and public sector entities rely upon the regime as a primary means of identification.[21] The existence of a robust, queriable system incentivizes private sector adoption for a greater variety of value-added services, which in turn can fuel greater enrollment and increase coverage rates. In this way, a virtuous cycle of enrollment can be established with the proliferation of use cases in the private sector. Consistent, long-term policy commitment is necessary to achieve coverage rates sufficient to produce these compounding benefits.

## Robustness and Accuracy

Private sector firms rely on identification systems to verify the uniqueness of a given individual, establish the truth of relevant attributes such as name and address, and confirm that customers are, in fact, who they claim to be. For that reason, the potential benefits of an identification system for the private sector depend on the overall robustness of the system—i.e., the accuracy, integrity, and security of its data and credentials.

The **accuracy** of identity data is particularly important in a private sector context, where the costs of fraud and inaccuracy are diverse and far-reaching. First, data must be correct for the person in question. That is, information must not only be true, but accurately matched to the proper individual. This trait is bolstered by the presence of a unique identifier that facilitates deduplication, but also requires efficient and precise enrollment processes to ensure that records are matched inextricably to the appropriate subjects. Second, the data in an information system must be correct *at that time.* This requires dynamic updating of identification systems such that an individual's record within the system reflects personal data as it changes over time. Database harmonization within the public sector assists in achieving this goal.

---

20 For additional information on the definition and components of a legal identity, see "Principles on Identification for Sustainable Development: Toward the Digital Age." World Bank, February 2017.

21 "Identity for Development in Asia and the Pacific." Asian Development Bank, 2016.

The cost of inaccurate personal data in the private sector is manifested in several ways. Issues related to fraud, mispricing, and narrowed customer bases are prevalent across various industries. More broadly, a third of business leaders simply do not trust the data they use in decisionmaking, and poor data quality is estimated to cost the American economy over 3 trillion dollars per year.[22] Accurate personal data provided by an authoritative identification system would considerably reduce that cost and allow for more efficient provision of services across industries.

22 "The Four V's of Big Data," IBM Big Data & Analytics Hub.

# 3. Primary Economic Impact Channels in the Private Sector

Evidence suggests that identification systems characterized by the features and conditions outlined above can create three primary channels for economic impact across the private sector. Two channels are shared with the public-sector analysis in this area: robust systems with high coverage can (1) decrease costs and expenditures as well as (2) increase revenues as compared pre-implementation levels. An additional channel, (3) facilitating a more "business-friendly" economy, is included here as a means of analyzing broader cross-sector market impacts within a given country.

Several specific savings and revenue generation mechanisms exist within each of these three broader channels, though policy makers should not anticipate that the relative size of these channels will be consistent across industries and identification system types. In addition, it is possible that additional forms of savings or revenue generation beyond those mentioned here may develop as identification systems mature, and additional second- and third-order effects may contribute to even greater levels of economic impact. In order to provide a more complete picture of the economic relationship between government-provided identification systems and the private sector, this section also briefly examines potential negative economic impact channels that may result from changes in identification systems.

## Savings Channel: Decreasing Costs and Expenditures

### Reduced Administrative and Transaction Costs

In the absence of a reliable, digital, government-recognized identification system, or where only legacy paper-based systems exist, both customers and private service providers bear a number of transaction costs throughout the private sector identity lifecycle.

In industries that require a high degree of identity assurance or regulatory compliance (e.g., financial services, mobile/telecommunications, sharing economy, etc.) some degree of identity verification is required as part of the onboarding process for a new customer. If potential customers possess no authoritative identity credential, they may be denied the opportunity to purchase that service entirely (this phenomenon is explored in more detail in the revenue generation section). If the country in which they reside only provides paper-based identity credentials, onboarding requires customers to visit a branch or office in person to apply for a desired service. This adds additional time and monetary costs for consumers that may act as a barrier to accessing desired services. Such in-person visits are also more expensive transactions for service providers than digital or phone-based interactions. In financial institutions, for example, the average cost of an in-person transaction is around $4.25, while mobile transactions reduce that figure to only $0.10.[23] In this way, the lack of a digital identity represents a direct cost inefficiency to service providers and consumers alike.

23 "Mobile Banking Adoption: Where Is the Revenue for Financial Institutions?" Fiserv White Paper, 2016.

## Table 2: Identification System Features Enabling Decreased Private Sector Costs and Expenditures

| 1. Decreased Costs and Expenditures | | | | | |
|---|---|---|---|---|---|
| *Pathways* | *Features of Identification System* | | | | *Conditions* |
| a. Reduced administrative and transaction costs | Digitization | Unique ID | Integration/ Interoperability | Queriability | • Coverage<br>• Robustness and accuracy |
| b. Reduced theft and fraud | | Unique ID | Integration/ Interoperability | Queriability | • Coverage<br>• Robustness and accuracy |
| c. Reduced compliance costs | Digitization | Unique ID | Integration/ Interoperability | Queriability | • Coverage<br>• Robustness and accuracy<br>• Clear, consistent regulatory structure |
| d. Reduced liability costs | | | | Queriability | • Coverage<br>• Robustness and accuracy<br>• Clear, consistent regulatory structure and framework for recourse |

Onboarding also requires identity verification procedures in order to evaluate counterparty risk, credit risk, or fraud risk, depending on the industry. Where no queriable identification system exists, companies may have to collect and store paper-based personal information, manually evaluate customers, and solicit ad hoc means of proving identity attributes, like utility bills or pay stubs. This can be a time-consuming, inaccurate, and expensive process. While a robust, high coverage identity system does not eliminate the need for rigorous onboarding processes, it does ease the cost and time burdens for onboarding and initial service applications across industries. Norway's BankID, for example, was able to reduce the time associated with applying for university housing from 10–14 days to 1–3 days.[24]

In India, for example, the Aadhaar system offers clear opportunities for savings by allowing third parties to authenticate the identity of users and (in select cases) remotely and securely verify a limited set of attributes.[25] Before the system was implemented, the average Indian firm's onboarding cost was about 1,500 rupees, or around $23. With the increased queriability, digitization, and interoperability of the Aadhaar system, some estimates indicate that onboarding costs could plummet to as little as 10 rupees,

24 GSMA 2014.

25 See https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf for more information on the new "limited eKYC" policy.

or approximately $0.15.[26] For a single company like Uber, which has an estimated 240,000 drivers that have undergone verification for onboarding, that means Aadhaar could feasibly have produced savings of nearly 358 million rupees, or close to $5.5 million for one company alone.[27]

> The Aadhaar digital identity system could reduce onboarding costs for Indian firms from 1,500 rupees to as low as an estimated 10 rupees.

Identity-based transaction costs are not limited to onboarding, however. Authentication throughout a customer's lifecycle with a company also represents a significant cost, which is exacerbated where no queriable identification systems are available. Around 30 percent of calls to banks' call centers, for example, are requests for account access due to misplaced or forgotten passwords. Each one of these interactions costs a company about $25.[28] Lack of uniqueness in customer records are also costly for companies and potentially risky. In the U.S. health care sector, for example, duplicate records cost medical institutions $1,000 each, plus an additional $5,000 to correct the record.[29] With more immediate access to authoritative digital identification systems, these costs could be substantially mitigated. Digitization of general business processes can save enterprises an estimated 90 percent over existing practices, with the assurance of trusted identity credentials offering further targeting savings.[30]

### Identity in the Travel Sector

**Case Study Snapshot: United Arab Emirates (UAE)**

The travel industry is valued at some $2.7 trillion globally[31] and served over 3.8 billion air travelers in 2016—a number that is expected to reach 7.2 billion by 2035.[32] The identity of each of these individual travelers must be verified multiple times throughout their journey, including during ticket purchase, check-in, security checks, and (if crossing borders) immigration and customs. However, the paper-based passports and other identity documents that underpin these verifications are often expensive and inefficient.

Customer abandonment rates are high in online purchases, often stemming from friction in identity verification and authentication processes.[33] Research has indicated that airlines themselves accrue overhead costs and fines of about $0.50 per passenger,[34] and errors in passenger identity data are

26 "Indian business prepares to tap into Aadhaar, a state-owned fingerprint-identification system." *The Economist,* 24 December 2016.
27 "India's Uber drivers feel taken for a ride on earnings promises." *The Financial Times,* 25 March 2017.
28 "The Future of Identity in Banking" Accenture White Paper, 2013.
29 "Strategies for improving patient identification and patient record integrity." Imprivata White Paper, 2017.
30 "Accelerating the digitization of business processes," McKinsey & Company, May 2014.
31 "Transforming the Airline Passenger Journey," OIX UK, September 2017.
32 "IATA Forecasts Passenger Demand to Double Over 20 Years," International Air Transport Association Press Release, 18 October 2016.
33 "Why almost 50% of your customers abandon online transactions," Experian, 30 October 2014.
34 "Transforming the Airline Passenger Journey," OIX UK.

a prominent factor. Furthermore, the high cost of documents—e.g., a passport costs more than 10 percent of per capita income in 10 percent of countries—may be insurmountable to some would-be travelers, creating a significant barrier to free movement and shrinking the potential customer pool.[35] Improved identification systems thus represent a massive financial opportunity in the travel sector.[36]

As home to the third busiest airport in the world by passenger volume—nearly 84 million passengers passed through Dubai in 2016[37]—the UAE is a prime example of a country that has benefited from leveraging its digital identity platform to streamline identity verification processes in the travel industry.[38]

In June 2017, the UAE released a digital Smart Wallet app that can replace paper-based identity documents for travel. In the current "phase one" iteration, customers can upload existing passport and visa information to the app. At the airport gate, the app produces a bar code to be scanned, eliminating the need for passengers to produce physical identity documents. The service can be used by all national ID holders ages 18 and above, and over half a million travelers have taken advantage of the service thus far.[39] The digital verification process is estimated to have reduced the time required for identity checks by airlines to 9–12 seconds, creating significant savings in administrative costs. In the future, the UAE has plans to expand the range of Smart Wallet services outside the travel sector to improve the ease of verification for a variety of public and private sector services.[40]

In addition, the government has announced the development of a "biometric border" in Dubai's airport, which will replace smart gates with facial recognition scanners that can detect and verify a traveler's identity. These developments thus far only apply to those with a UAE digital identity, but other countries and airlines around the world (e.g., JetBlue flights to Aruba[41] or KLM in Amsterdam[42]) are investigating similar mechanisms for cost reduction and time savings during air travel.

## Reduced Theft and Fraud

The role of robust identification systems in onboarding and customer verification is also central to preventing theft and fraud. Identity theft has been the top consumer complaint to the U.S. Federal Trade Commission (FTC) every year for the past 15 years. Approximately 15.4 million Americans were the victims of identity fraud in 2016, with losses totaling $16 billion.[43] Worldwide identity theft costs are estimated to be at least $221 billion.[44] While robust identification systems cannot fully eliminate losses due to theft,

35 McKenzie, David, "Paper Walls are Easier to Tear Down: Passport Costs and Legal Barriers to Emigration." World Bank Policy Research Working Paper 3783, December 2005.

36 Notably, although the ability to effectively prove one's identity is a cornerstone of the industry, travel is also one of the most difficult sectors in which to implement effective digital systems. It is governed by a web of national and international governance mechanisms as well as private sector infrastructure and service providers, making implementation of any uniform policy arduous. Travel also involves crossing borders, which means the industry straddles sensitive, highly regulated, and intersecting interests in national security and immigration.

37 "Here are the 20 busiest airports in the world," *Business Insider,* 17 May 2017.

38 Al-Khouri, Ali M., "Connected Government: An Exploration of the UAE's Identity Management Integration Strategy." Macrothink Institute, 1 April 2013.

39 "New smart gates set to cut queues at Dubai airport," *Gulf News,* 24 September 2017.

40 "Now, smartphone is your passport in Dubai," *Gulf News,* 7 June 2017.

41 "JetBlue Replaces Boarding Passes with Facial Recognition Tech." WBUR Boston, 19 June 2017.

42 "KLM Tests Facial Recognition to Ease Boarding Without Passes." Bloomberg Technology, 8 February 2017.

43 "2017 Identity Fraud: Securing the Connected Life," Javelin Strategy & Research, February 2017.

44 "How to Prevent and Detect Business Identity Theft," U.S. Small Business Association, January 2013.

fraud, and other economic crime, they can increase security for private companies in numerous industries and help firms avoid redress costs when businesses or customers are defrauded.

First, strong identification systems with efficient query mechanisms can help firms gauge customer fraud risk before a transaction has taken place. The ability to accurately identify a consumer during onboarding and correlate that verified identity with previous financial behaviors through digital processes creates transaction efficiencies and can help prevent future fraud losses. Later in the customer identity lifecycle, trusted digital credentials can help mitigate fraud at the point of transaction. In Malaysia, for example, the majority of banks possess a MyKad card reader to provide real-time identity authentication by directly querying government-backed personal and biometric data stored on the card.[45]

Second, synthetic identity fraud can also be mitigated through mature identification systems that have high levels of integration and queriability. In the United States, for example, the social security number (SSN) has a low degree of queriability and the private sector has historically relied on other third-party providers to verify or authenticate SSNs. This has contributed to the massive (and likely growing) problem of synthetic identity fraud, in which malicious actors combine attributes from different real identities—e.g., one person's name, a different person's SSN, and the address of a third—to create a fictional identity.[46] Currently, fraud committed by consumers using synthetic identities is growing: up to 20 percent of defaulted credit card debt may already be the result of synthetic identity fraud, and the technique costs lenders worldwide an estimated $6 billion in 2016.[47]

> Queriable identification systems can help mitigate synthetic identity fraud, the cause of an estimated 20 percent of credit losses.

Third, high levels of interoperability between a national-level identity system and private industry can facilitate streamlined federation of identity credentials at a customer's request. Ensuring that service providers and government agencies possess identical, timely, and accurate information can produce positive network effects contributing to overall levels fraud prevention throughout the economy in a given jurisdiction. In Finland, for example, mobile identity providers have established a "circle of trust" within which digital identities can be transferred according to consumer preference. Additional private sector service providers from other industries have joined this trusted platform, with further expansion of services likely in the future.[48]

## Reduced Compliance Costs

Industries with targeted regulatory frameworks are particularly susceptible to cost burdens resulting from underdeveloped identification systems. This is especially true of financial services, payments, mobile technology and services, and health care, for example, though nascent industries like the sharing economy are likely to attract additional regulatory attention in the near term. Pressures to accurately verify and authenticate customer data stem not only from internal business mandates to avoid fraud, theft, or default risk, but also from governments attempting to deter money laundering and other criminal activity and foster broader economic stability.

---

45 "Identity for Development in Asia and the Pacific." Asian Development Bank, 2016.

46 A recent example of this concern comes from the 2017 Equifax breach in the United States. For more information, see https://www.bloomberg.com/news/articles/2017-09-08/equifax-s-historic-hack-may-have-exposed-almost-half-of-u-s.

47 "Synthetic Identity Fraud Cost Lenders $6 Billion in 2016: Auriemma Consulting Group." ACG, 1 August 2017.

48 Murphy, Alix, "Finnish Mobile ID: A Lesson in Interoperability." GSMA Case Study, February 2013.

Regulatory compliance is a significant business expense for high-trust industries in all regions. In Asia, for example, banks alone report budgeting $1.5 billion annually for AML compliance activities.[49] In Europe, KYC costs the average bank $60 million per year, with individual transactions ranging from £10 to £100 ($13.40 to $134) per identity check. By 2020, a typical bank in the UK will waste £10m ($13.4 million) every year on inefficient, manual verifications as part of KYC processes.[50] More broadly, some financial firms are spending up to $500 million per year on consumer due diligence (CDD) and KYC compliance.[51]

> By 2020, the typical UK bank will spend over $13 million per year on inefficient KYC processes—costs which can be mitigated significantly by robust, queriable, digital identification systems.

Fines for violating KYC, AML, or broader CDD regulations also pose a sizable risk for firms in these high-trust industries. HSBC, for example, was fined nearly $2 billion in 2012 and BNP Paribas was ordered to pay $8.9 billion in 2014.[52] Beyond those headline-grabbing individual cases, industry professionals expect the regulatory climate to continue to tighten in 2017 and beyond. With the General Data Protection Regulation (GDPR) looming in the European market, 60 percent of finance professionals expect the personal liability of compliance officers to increase over the next year, and 70 percent are expecting the number of regulatory guidelines issued to continue to increase.[53]

In some cases, governments are seeking to directly integrate KYC and other compliance functionality into burgeoning foundational identity systems. The Unique Identification Authority of India (UIDAI), for example, has built IndiaStack, a set of APIs to facilitate verification of the country's Aadhaar personal identifier for private sector use cases. To date, IndiaStack has allowed for nearly 3 billion identity authentications for private transactions, including completing 150 million distinct digital KYC reviews and linking 339 million bank accounts with Aadhaar numbers.[54] Singapore has also begun bolstering the queriability of its burgeoning national identity system, linking all 3.3 million users of its public sector federated identity credential with its private-sector integrated MyInfo service by the end of 2017.[55]

Malaysia, Thailand, and several other countries are also drafting legal standards to govern identity verification for streamlined electronic KYC (eKYC) protocols.[56] With these standards in place, private sector companies will be able to more easily access the source of truth in identity credentials (that is, the government's identity records) and, assuming a basic level of digitization and queriability, be able to remain compliant with greater ease. Though this level of integration is still nascent even in the most mature identification systems around the world, it is likely that this phenomenon will translate into a reduction in spending on inefficient compliance mechanisms and a reduction in identity-verification-based compliance penalties.

---

49 "Uncover the True Cost of Anti-Money Laundering & KYC Compliance." LexisNexis Risk, 2016.
50 "AMLD4/AMLD5 KYCC: Know Your Compliance Costs." Consult Hyperion, June 2017.
51 "Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity." Thomson Reuters, 9 May 2016.
52 "BNP Paribas to pay record US $8.9-billion fine for facilitating transactions in sanctioned Iran, Sudan and Cuba." Financial Post, 30 June 2014.
53 "Cost of Compliance 2016." Thompson Reuters, 2016.
54 See http://indiastack.org/about/.
55 "More convenience for all SingPass users by year-end." Today Online, 27 September 2017.
56 See https://globalcompliancenews.com/electronic-know-your-customer-e-kyc-anti-money-laundering-in-digital-era-20160915/ and https://www.nst.com.my/business/2017/09/276402/bnm-finalise-standards-e-kyc for more detailed information on eKYC development in Malaysia and Thailand.

## Reduced Liability Costs of Holding Personal Data

Closely related to compliance costs are the financial burdens of holding, maintaining, and securing stores of customers' personal data for identity use cases. Where no robust, queriable identification system exists, firms may be forced to rely on internally developed processes to collect customers' personal data for the purposes of initial verification, as well as authentication and authorization throughout the customer's lifecycle.[57] This requires not just the collection of personal data, but securely holding it and, when necessary, disposing of it. Liability concerns are especially pertinent when companies fail to maintain high standards for data protection and privacy. In the context of increasingly high-profile and damaging hacks and leaks of personal data online, the possession of sensitive identity data is in itself a risk to private sector firms that can be mitigated through leveraging robust, government-backed identification systems.

Though potential liability costs are difficult to quantify before personal data is actually compromised, there are a few quantitative metrics that can serve as a proxy for this type of risk. First, major corporations now purchase cyber insurance to shield their businesses from loss in the event of a breach. Premiums vary widely based on the size of the corporation, the type of data protected, and the cyber infrastructure the firm already has in place.[58] However, as the size and number of data breaches expands, insurers are struggling to properly price policies. U.S. retailer Target had a $100 million policy when it fell victim to a security breach in 2013 that led to losses of over $450 million.[59]

Another means of assessing data liability costs in the private sector is to examine regulatory penalties for the misuse of personal data. Many jurisdictions still have relatively underdeveloped legal frameworks for data protection. The forthcoming implementation of GDPR in the European Union (EU), however, will be a valuable test case. The law has a tiered system of fines for companies that fail to adequately protect identity data with a maximum penalty of €20 million ($23.63 million) or 4 percent of global annual turnover from the previous year, whichever is greater. The law applies to all companies who hold or process personal information from EU citizens. For a large international corporation, 4 percent of global turnover is a significant portion of revenue.[60]

Government-backed identification systems cannot halt cybercrime or guarantee that personal data will not be put at risk. However, if private corporations can minimize the personal data they hold and rely instead on querying a trusted government system, the risk and potential costs of corporate data breach can be mitigated. In this way, creating a robust identification system can ease potentially massive liability costs across a given market.

# Revenue Channel: Increasing Revenue Levels and Revenue Generation Opportunities

## Increased Customer Base

Lack of legal identity is a fundamental impediment to a person's participation in the formal economy. Of the estimated 2 billion unbanked adults worldwide, 360 million—nearly a fifth—are unable to access the

---

57 For many industries, customer-facing firms will hold identity data for various business purposes outside of identity verification and authentication use cases. For that reason, companies internally develop systems to collect and manage personal data for reasons unrelated to the identity ecosystem in which they operate.

58 For a range of premium levels by industry and annual revenue, see https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/.

59 "The Cost Of Cyber Breach—How Much Your Company Should Budget." *Forbes,* 19 April 2017.

60 For more on the specific provisions of GDPR, visit http://www.eugdpr.org/.

## Table 3: Identification System Features Enabling Increased Revenue Generation Opportunities

| 2. Increased Revenue Generation | | |
|---|---|---|
| *Pathways* | *Features of Identification System* | *Conditions* |
| a. Increased consumer base | Digitization; Unique ID; Queriability; Private Sector Cooperation | • Coverage<br>• Robustness and accuracy |
| b. Decreased consumer abandonment and rejection | Digitization; Unique ID; Integration/ Interoperability; Queriability | • Coverage<br>• Robustness and accuracy |
| c. Fees charged for identity services | Digitization; Private Sector Cooperation | • Coverage<br>• Robustness and accuracy |

formal financial sector due to insufficient identity documentation.[61] That means a consumer pool greater than the population of the United States could be created if these unbanked individuals were to gain access to trusted identity credentials. As the number of "identified" individuals within a given market increases, the customer base available to firms across industries expands, creating enormous additional revenue generation opportunities.

### Identity in the Mobile Sector

**Case Study Snapshot: Pakistan**

Identification is vital to the mobile and telecommunications industry, not only due to their need to identify customers as part of their core business processes, but also because they provide mobile identity platforms and services to other industries and sectors. Mobile technologies and services generated $3.3 trillion (about 4.4 percent of global GDP) in 2016,[62] and the mobile identity management market is expected to grow at an annual rate of nearly 10 percent.[63] Streamlined identification infrastructure therefore has the potential to generate massive economic opportunity.

High levels of mobile penetration can also form the foundation for mobile financial services, payments, and e-governance opportunities. Mobile banking, for example, can lower the cost of financial services provision by 80–90 percent.[64] Especially as relatively basic cell phones are equipped with biometric

61 World Bank's 2014 Global Findex.
62 "The Mobile Economy 2017." GSMA, 2017.
63 "Global Mobile Identity Management Market 2016-2020." Technavio, September 2016.
64 McKinsey Global Institute, September 2016.

devices to facilitate unique authentication processes (i.e., camera, fingerprint scanner), mobile service providers operate an important gateway to expanded digital identity services.

The development of Pakistan's Computerized National ID Card (CNIC) and its relationship with mobile finance illustrates these mutually reinforcing goals of identity ecosystem development and mobile sector growth. In 2014, the Government of Pakistan mandated that all SIM card registrations be verified with biometric data drawn from the country's national ID system, managed by the National Database and Registration Authority (NADRA). This integration proved to be a turning point for the expansion of mobile industry development in the country.

A few key contextual factors made Pakistan an especially promising area for mobile development facilitated by digital identity. First, most citizens already carried a CNIC, which included coded fingerprint data along with additional personal information. Requiring CNIC registration for SIM cards created a positive network effect, allowing the CNIC system to enroll the last 10 percent of Pakistani citizens who had previously lacked an identity.[65] Second, Pakistan had very low levels of financial inclusion. In 2014, only 13 percent of the adult population in Pakistan had access to formal financial services, including just 5 percent of women. The mobile penetration rate was comparatively high, however, reaching nearly 50 percent of the total population.[66]

Telenor, at the time the second largest mobile network operator in Pakistan, took advantage of the opportunity to expand its financial offerings through its Easypaisa payments service. The company successfully negotiated for the Bank of Pakistan to accept CNIC-verified SIM registration information as sufficient identity authentication for its own KYC purposes. This reduced onboarding time to under one minute, and allowed for Telenor to offer mobile money services to their customers at the point of SIM registration.[67]

In just over a year, Easypaisa's customer base doubled to nearly 5 million. The service now boasts 20 million users and processes the equivalent of 3 percent of Pakistan's GDP.[68] After having invested only $7 million in the initial creation and marketing of Easypaisa, Telenor estimates that financial services will constitute 10 percent of annual revenue.[69]

In the financial sector alone, digitization throughout the consumer lifecycle could bring an additional 1.6 billion customers from developing markets into the formal economy. Worldwide, this would generate 95 million new jobs across industries, create $4.2 trillion in new deposits and extend $2.1 trillion in new lines of credit, for an overall 6 percent boost in developing economy GDP by 2025.[70] These striking projections represent a combination of savings and revenue generation mechanisms. Not only does the presence of a trusted identity credential remove a barrier to economic participation, but highly queriable, digital systems lower onboarding and transaction costs, which in turn allow companies to expand service offerings to new populations.

---

65 "Digital Identity: a prerequisite for Financial Inclusion?" GSMA, 19 September 2016.
66 "Country Overview: Pakistan." GSMA, 2016.
67 For more information on mandatory SIM card registration in Pakistan, see the relevant case study in "Mandatory registration of prepaid SIM cards: Addressing challenges through best practice." GSMA, April 2016.
68 "Digital Identity: a prerequisite for Financial Inclusion?" GSMA, 2016.
69 Bjaerum, Roar, and M. Yasmina McCarty, "Easypaisa: Mobile Money Innovation in Pakistan." GSMA, July 2013.
70 "Digital finance for all: Powering inclusive growth in emerging economies." McKinsey Global Institute, September 2016.

Pakistan's Telenor leveraged the national ID and government-mandated SIM registration to reduce onboarding time and expand the customer base for its Easypaisa payments service, which now has 20 million users and processes the equivalent of 3 percent of Pakistan's GDP.

In addition to increasing customer bases through the overall extension of an identification system, companies that *partner* with the government to implement identification programs may have further opportunities. In Tanzania, for example, the country's Registration, Insolvency and Trusteeship Agency (RITA) and UNICEF partnered with telecom company Tigo in 2011 to build a five-year plan aimed at developing and deploying a mobile birth registration platform to address under-registration. Within the first six months of the local pilot program, the Tigo SMS-based mobile app registered 127,000 children, increasing registration rates from just under 9 percent to more than 30 percent.[71] Since then, the program has been extended and has registered almost 1.5 million children across seven regions in Tanzania.[72]

For Tigo, the program has provided an opportunity to expand its consumer base and develop additional advanced applications. This program alone will expose over 1,300 birth registration assistants and the hundreds of thousands of families with whom they work to Tigo services, including the popular Tigo Pesa mobile payment platform.[73] The birth registration app has also spurred the development of similar Tigo services in Ghana and Bolivia, building the company's brand in new and growing markets.

In Tanzania, Tigo partnered with UNICEF and the national government to develop a birth registration platform that has registered nearly 1.5 million children and broadened the company's consumer base in growing markets.

## Decreased Consumer Abandonment and Rejection

Increased availability of trusted identity information not only increases the absolute number of customers a firm can onboard, it also provides companies with tools to retain more customers and generate increased lifetime value per customer.

As discussed previously, onboarding and initial identity verification processes are both resource and time intensive for companies, especially in highly regulated industries. These inefficiencies increase friction for customers as well. The more arduous the verification process, the more likely customers are to abandon the transaction, either in favor of a more user-friendly experience, or by foregoing the service entirely. Abandonment rates vary widely by industry. In the UK, an estimated 25 percent of financial services applications are abandoned, for example, due to difficulties in the KYC process.[74] In e-commerce, that figure spikes by a factor of three, with most abandonments occurring during a login or payment verification process.[75]

---

71 "Innovations in Mobile Birth Registration: Insights from Tigo Tanzania and Telenor Pakistan." GSMA, January 2017.
72 "The Mobile Economy: Sub-Saharan Africa 2017." GSMA, 2017.
73 "Tigo continues to support mobile birth registration in Tanzania." Tigo Press Release, 24 March 2017.
74 Consult Hyperion, June 2017.
75 "E-Commerce retailers are losing their customers because of this one critical mistake." *Business Insider,* 16 March 2016.

Accurate, highly queriable identification systems can reduce these attrition rates by over 80 percent in some industries. By leveraging broad coverage rates and robust digital queriability, one South Korean mobile identity authentication provider was able to decrease customer abandonment for a mobile gaming site from 24 percent to just 4 percent. In addition, it was able to streamline authentication for fund transfers, reducing transaction times from 90 seconds down to 15 seconds.[76]

> A South Korean mobile identity authentication provider was able to reduce financial transaction times from 90 to 15 seconds by leveraging broad coverage rates and robust digital queriability.

Robust, queriable identification systems can also help private organizations more accurately gauge fraud risk, leading to fewer false positives (i.e., incorrectly assigning a high fraud risk score to a customer) and rejected transactions due to inaccurate verification. Surveys have shown that false customer rejections are actually costlier to firms than fraud over the lifetime of a customer. In the U.S. online retail market, for example, companies lose $118 billion in revenue in a given year due to unwarranted transaction rejections, as compared to $9 billion in measured fraud. Merchants estimate that between 2.5 and 5 percent of transactions are declined, and 10 percent of those are false. Moreover, once falsely declined, a third of prospective customers never engaged with that merchant or service provider again.[77]

## Fees for Identity-Related Services

An additional opportunity for revenue generation in the private sector results from the ability of firms directly involved in providing government-backed identification systems—i.e., through a PPP—to charge fees for identity services. This has the potential to create revenue streams both from per-transaction fees themselves and from add-on services.

The South Korean mobile identity authentication provider mentioned above, for example, has developed a fee-per-query model for providing trusted digital authentication for $0.04 per transaction. While this figure seems low in absolute terms, the sheer volume of identity-related transactions makes this a significant revenue source. This company has nearly 5.5 million individual users who, through the platform, can have their identity authenticated with nearly 27,000 businesses and service providers. At approximately 62 million unique authentications per month, this single identity service may generate nearly $30 million in annual revenue.[78]

> By charging $0.04 per transaction for 62 million unique authentications per month, one South Korean mobile identity authentication provider could generate nearly $30 million in annual revenue.

76 Based on e-mail correspondence between source and One World Identity on September 22, 2017. The source requested to remain anonymous.

77 "Fixing Retail's $118B Mistake." PYMTS.com, 8 October 2015.

78 Based on e-mail correspondence between source and One World Identity on September 22, 2017. The source requested to remain anonymous.

SK ID Solutions, the Estonian government's partner in issuing certificates for national identity documents, operates on a fee-per-query basis as well, serving more than 700,000 end users in the country. It offers multiple identity-related services priced by transaction, from 0.007€–0.10€ ($0.01–$0.12) depending on volume.[79] The Danish NemID program also generates significant revenue for its PPP identity authentication system. Through the NemID platform, citizens can use a common digital identity to access both government services and secure private transactions like payments. In 2016, system implementation directly "delivered strong growth" to the Nets Group, the private firm operating the platform.[80]

Full transparency on revenue information and pricing models for these services is not commonly available, but it is clear from these examples and the proliferation of maturing digital identification systems in markets around the world that this will continue to be an expanding channel for private sector revenue moving forward.

### Identity in Financial Services Sector

**Case Study Snapshot: Sweden**

Identity is key to use cases throughout the customer lifecycle in the financial services industry, and banks currently spend over $1 billion annually on identity management solutions.[81] Numerous savings and revenue generation opportunities arise in the private sector from improved government-provided identification systems.

Moreover, because robust identity verification and authentication mechanisms are required in this industry, financial services providers themselves often serve as providers of federated identities for other transactions, as with Norway's BankID, Denmark's NemID, and GOV.UK Verify. Some have argued that financial institutions are uniquely qualified to serve as foundational identity providers as digital identity regimes around the world mature.[82] The development of BankID in Sweden provides a valuable illustration of financial services in identity system architecture, and the multiple economic impact channels that dynamic can facilitate.

Sweden has a long history of robust federal identity ecosystem. Swedes have had a foundational identification system characterized by a unique ID number since 1974, allowing administrative frameworks and the broader public to adapt relatively easily to digitization. The Swedish government opted to pursue a market-based digital identification system rooted in the financial services sector to spur competition between identity service providers, thus facilitating innovation and driving per-transaction costs down, creating trusted identity integrations into a greater variety of e-services, and reducing initial implementation costs for the public sector.[83]

First launched in 2003 and managed by a consortium of 10 Swedish banks, BankID is a PPP-based identification system. All customers of participating banks are given an eID free of charge, which

79 Price lists available at https://sk.ee/en/services/pricelist/certificate-validation-services.

80 See full Nets Group Q4 2016 financial report at https://investor.nets.eu/-/media/Files/N/Nets-IR/documents/Financial-results-for-Q4-2016.pdf.

81 "The future of identity in banking," Accenture, 2013.

82 For a comprehensive report on the role of financial institutions in digital identity system development, see "A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity." World Economic Forum, August 2016.

83 Grönlund, Åke, "Electronic identity management in Sweden: governance of a market approach," Identity in the Information Society, Volume 3, Issue 1, pp 195–211. July 2010.

can be used to authenticate transactions across the private and public sector. Companies looking to integrate BankID with their services establish a contract with a bank in the BankID network, facilitating an additional direct revenue stream to participating financial services institutions. Identity credentials themselves are available in "hard" form—encoded on a smart chip—or "soft" form, which is available on a user's personal computer, tablet, or phone.[84] Currently, BankID facilitates 2 billion transactions per year and is used by more than 80 percent of Swedish citizens.[85]

Sweden has additional plans for the program's continued expansion, as well. BankID has recently integrated next generation identity verification and authentication mechanisms based on behavioral biometrics to minimize reliance on passwords.[86] Six of the country's largest banks also cooperatively launched a common mobile payment app, Swish, in 2012, building on BankID's functionality. As of 2014, the app had expanded its services to include e-commerce payments at a cost of 1.5 and 2 kronor ($0.19–$0.25) per transaction for retailers.[87] Swish is now used by more than five million Swedes for real-time digital payments, with a user base growing by over 150,000 per month. These advanced and improving levels of digitization, innovation, and reliable identification infrastructure have secured Sweden's status as one of the top 10 countries in terms of "ease of doing business."[88]

## Economic Climate Channel: Facilitating Economic Development through "Business Friendly" Policies

**Table 4: Identification System Features Enabling the Development of a "Business Friendly" Economic Environment**

| 3. Economic Climate | | | | | |
|---|---|---|---|---|---|
| *Pathways* | *Features of Identification System* | | | | *Conditions* |
| Overall "business friendly" ecosystem | Digitization | Unique ID | Integration/ Interoperability | Queriability | • Coverage<br>• Robustness and accuracy<br>• General effectiveness of economic governance |

A final economic impact channel of identification systems to the private sector is facilitating a generally "business friendly economy." Although this is considerably more abstract and difficult to quantify, the relatively diffuse nature of benefits in this channel, governments, and private firms should not discount potential impact in this area. Identification systems are crucial tools for accomplishing political, economic, and human development goals (indeed, legal identity is itself among the United Nations' Sustainable

84 For additional information on the BankID platform, see https://www.bankid.com/en/om-bankid/detta-ar-bankid.
85 "ISSE 2016: The four models of digital identity," SC Media UK, 23 November 2016.
86 "Google plans to kill passwords with this tech, but Scandinavia is way ahead of it," Quartz, 31 May 2016.
87 "Swedish banks want to use Swish for ecommerce." Ecommerce News—Europe, 27 January 2015.
88 World Bank Ease of Doing Business Index 2017.

Development Goals).[89] Implementation of robust and inclusive identification systems also tends to be correlated with broader levels of effective governance.[90] Simply put, strong identification systems are at the core of mutually reinforcing development dynamics that can benefit the broader economy.

Estonia's ubiquitous digital identity infrastructure is a prime illustration of this relationship. Currently, Estonia is one of the most business-friendly economies in the world, ranking 12th in the world in terms of "ease of doing business."[91] The country's advanced digital infrastructure has made it an attractive corporate market for years, but with the institution of Estonia's e-residency program—which allows anyone in the world to apply for an Estonian government-issued digital ID—even greater opportunities for revenue generation have emerged.[92] Since the program launched, e-residents have established over 1,300 distinct companies and have contributed over €4.3 million ($4.6 million) in both taxes and services to the Estonian economy.[93] The robust identification system underpinning the e-residency program has thereby directly facilitated the creation and registration of new businesses in Estonia. Moreover, applications for e-residency spiked after the UK formally began the process of leaving the EU, indicating that Estonia's corporate culture will continue to attract investors and business owners alike.[94]

> Estonia's e-Residency program—underpinned by a robust digital identification system—has led to the creation of more than 1,300 new companies by e-Residents, bringing an additional $4.6 million into the Estonian economy.

Anecdotal evidence also indicates that a business-friendly economy underpinned by mature identification systems may contribute to attracting elevated levels of international investment in both startups and more mature firms. In India, for example, startup funding in 2017 is on pace to more than triple the previous year's levels.[95] Estonia, too, has seen investment levels increase as its identity regime has matured.[96] Although the correlation between investment and the development of identification systems does not imply a causal relationship, the ability to accurately identify customers, mitigate fraud risk, and reach new markets of trusted users and partners is likely to factor into corporate decision making.

89 For full list of the Millennium Development Goals, see https://sustainabledevelopment.un.org/post2015/transformingourworld.
90 "Identity for Development in Asia and the Pacific," Asian Development Bank, 2016.
91 World Bank Ease of Doing Business Index, 2016.
92 See https://e-resident.gov.ee/ for more information about e-residency.
93 "Estonia has 1.3 million people: Here's how it plans to get 10 million e-residents by 2025." ZDNet, 20 March 2017.
94 Rang, Adam, "e-Residency applications from the UK are arriving twice as fast post-referendum." Medium.com, 27 March 2017.
95 "India Tech: Early-Stage Activity Dominates As The Industry Develops." CBInsights, 22 June 2017.
96 "Estonia: Foreign Investment." Santander, September 2017.

# 4. Potential Negative Economic Impact Channels

Despite the many benefits of robust and inclusive identification system for the private sector, there are a handful of ways in which such systems may also have negative economic impacts for firms, particularly in the short term. As with any new regulatory or technological framework, private firms must be cognizant of the integration and maintenance costs associated with the technical implementation of a new identification system. In the Pakistan case study cited above, for example, mobile network operators were required to purchase biometric readers and re-register all customer SIM cards against CNIC within 100 days at considerable up-front cost.[97] For Jamaica's 2017 project to launch the National Identification System (NIDS), $5 million out of $68 million in funding received from the Inter-American Development Bank was dedicated to "streamlined identity verification for [the] public and private sector," and an additional $600,000 was earmarked for improving "institutional capacity and [creating] linkages between the private and public sectors."[98]

Compliance with emerging identity-related regulations can also impose costs on the private sector, as companies must adapt to new legal structures, data storage protocols, and information access and sharing procedures. In advance of GDPR for example, the EU's largest companies expect to spend between $28 and $48 million to bring their businesses into compliance with the new data protection infrastructure.[99] This figure does not include penalties for compliance errors, which, as previously mentioned, could amount to €20 million ($23.63 million) or 4 percent of annual global turnover, whichever is greater.

Governments implementing new identification systems should thus craft policy frameworks and information technology guidelines with an eye toward flexibility, scalability, and, where possible, open identity standards, in order to help private companies recover some of the initial capital investment and longer term operational costs of identification system integration.[100] With consistent policy and effective communication between the public and private sectors, however, aggregate costs of integration and maintenance will almost certainly be lower than the development of private sector systems, as some sector specific studies have indicated.[101]

Inconsistent implementation and enforcement of national-level identity policies can also create economic inefficiencies with ramifications for the private sector. Numerous countries have abandoned identification systems at varying stages of development. Australia's protracted political debate over the Australia card, for example, continues to impact national attitudes toward identification systems generally, and specifically the emerging Govpass digital identity platform. The UK also abandoned its Identity Cards bill in 2010 after

97 "Pakistanis face a deadline: Surrender fingerprints or give up cellphone." *Washington Post,* 23 February 2015.

98 For a full profile on this status of Jamaica's NIDS project, see http://www.iadb.org/en/projects/project-description-title,1303.html?id=JA-L1072.

99 "Survey: 61 percent of companies have not started GDPR implementation." International Association of Privacy Professionals, 7 June 2017.

100 For more information on technology risks of identity system implementation, see "Identification for Development: Strategic Framework." ID4D, 25 January 2016.

101 See, for example, U.S. National Institute of Standards & Technology Planning Report 13-2, which presents an economic analysis of potential identity verification systems for the U.S. Internal Revenue Service.

a change in government. Some £4.5 billion ($5.9 billion) had been slated for the program, and no refund was issued to the 15,000 UK citizens who had already paid £30 ($39) for the card.[102]

When substantial changes are made to identity-related systems and policies, sunk costs may be lost, and companies may face new short- or medium-term integration and compliance costs as well as new inefficiencies. Countries can begin to mitigate these potential costs by stimulating dialogue on proposed identification systems with the public and private sectors, and prioritizing clear, consistent communication with the private sector on emerging regulatory requirements.

102 "ID cards scheme to be scrapped within 100 days." *The Guardian,* 27 May 2010.

# 5. Conclusions and Recommended Areas for Further Research

Previous research has shown that robust identification systems with high levels of coverage can help achieve policy and sustainable development goals. In the public-sector companion to this paper, a framework was established for understanding fiscal impacts of identification systems on government agencies.[103] With this research, policy makers will be able to more effectively allocate resources to prioritize system features that are likely to produce the strongest public savings and revenue generating effects.

This paper has built upon the established public-sector framework to consider economic impacts that reach beyond the public sector and into private industry. National-level identification systems are capable of creating positive financial impacts for private companies, both through direct cost savings and revenue generation channels, as well as through more indirect benefits to a country's overall economic climate. A set of five key system features—digitization, unique IDs, integration and interoperability, digital queriability for verification and authentication, and public-sector participation in identification system architecture—have the potential to generate positive economic effects through those channels. As nascent digital identification systems mature and develop linkages with a greater array of private sector service providers, these impacts are likely to grow in the future.

This analysis has also revealed several potential avenues for future research that would benefit governments, the international donor community, and businesses alike. First, longitudinal studies of identification systems as they develop within a given country could produce more targeted insights into the economic impacts of a particular system over time. Second, the maturation of a greater variety of digital identification systems around the world could provide additional opportunities for comparative analysis of the savings and revenue generation channels across sectors. This would provide valuable quantitative evidence of the relative magnitude of economic impact channels on the private sector, allowing policy makers to make more informed and contextually appropriate choices in identification system architecture.

Finally, a more in-depth examination of identification systems that are capable of verifying attributes not just of people, but of entities (i.e., the New Zealand Business Number or Estonia's e-Business Registration system) could help differentiate economic impacts generated by more effective management of personal data as opposed to more effective business administration. The two traits are likely to coincide within a given country, but the distinction would be helpful in moving toward a more precise understanding of identity-related policy and its effects.

103 World Bank, 2018.

worldbank.org/id4d